

## I. COMUNIDAD AUTÓNOMA

### 3. OTRAS DISPOSICIONES

Consejería de Educación y Universidades

Universidad de Murcia

**1164 Resolución del Secretario General de la Universidad de Murcia (R-7/2017), por la que se establece y admite el sistema de identificación con la cuenta corporativa institucional como sistema de firma electrónica de los interesados en el procedimiento administrativo.**

Durante la última década, la Universidad de Murcia ha realizado un enorme esfuerzo, continuado en el tiempo, para la puesta en marcha, gestión y soporte de los sistemas de firma electrónica previstos en los apartados a) y b) del artículo 13.2 de la derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, junto a la implantación generalizada de la Tarjeta Universitaria Inteligente (TUI) como dispositivo de creación de firma en el conjunto de la comunidad universitaria, que ha redundado en un crecimiento exponencial de trámites electrónicos, documentos y expedientes administrativos electrónicos, con las mayores garantías de seguridad posibles.

Sin embargo, el uso de estos sistemas de firma electrónica, basados en certificados electrónicos reconocidos, implica la instalación y actualización frecuente de diversos componentes software en el entorno del usuario, que añaden un alto grado de complejidad tecnológica para aquellas personas que realizan un uso poco frecuente de estos sistemas y que, a veces, puede resultar disuasorio y no siempre necesario, en virtud del principio de proporcionalidad, en aquellos trámites que no requieran un nivel de seguridad alto.

Por otro lado, la reciente Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 10.3, posibilita la admisión de sistemas de identificación como sistemas de firma electrónica para los interesados en el procedimiento administrativo, cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los mismos.

La Universidad de Murcia dispone de un sistema de identificación basado en la cuenta corporativa de correo institucional y su contraseña asociada -en adelante Cuenta UM-, que se adecúa a los criterios del apartado c) del artículo 9.2 de la citada Ley 39/2015, en cuanto al registro previo de los usuarios y al uso de claves concertadas, además de tratarse de un sistema plenamente implantado y aceptado por la mayor parte de nuestra comunidad universitaria para el acceso a multitud de servicios electrónicos, con lo que se presenta como una oportunidad en simplicidad y agilidad para ser utilizado como sistema de firma electrónica, siempre que se implanten medidas de seguridad adicionales que, por un lado, provean de un nivel de seguridad sustancial en la calidad de la identificación y, por otro, prevengan de un posible repudio de la actuación administrativa por parte del interesado.

En este sentido, la Resolución del Rector (R-638/2016), de 28 de julio, por la que se ordena la publicación del Reglamento de notificaciones electrónicas de la Universidad de Murcia, determina, en el apartado b) de su artículo 3, la posibilidad de utilizar la Cuenta UM junto a un código de un único uso generado, de forma no predecible, por la Universidad de Murcia y enviado al número de teléfono móvil asociado a la persona identificada, como método de identificación de nivel de seguridad sustancial.

Esta medida de seguridad, que se encuentra fundamentada en el uso de dos factores de autenticación (algo que se sabe -la contraseña asociada a la Cuenta UM- y algo que se tiene -el teléfono móvil donde se recibe el código de un solo uso-), se encuentra implantada en la Carpeta Ciudadana de la Universidad de Murcia para proteger el acceso a ciertos documentos administrativos de nuestros estudiantes, Personal de Administración y Servicios (PAS) y Personal Docente e Investigador (PDI), incluidos algunos tipos de las citadas notificaciones electrónicas, y se encuentra adecuada al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, que describe, en el punto 4.2.5 del apartado 2 de su anexo II, las medidas de seguridad a seleccionar para mecanismos de autenticación. Además, el punto 5.7.4 del mismo apartado, introduce la obligatoriedad, para sistemas de firma electrónica no basados en certificados electrónicos, de incorporar medidas compensatorias suficientes en lo relativo a la prevención del repudio, que ofrezcan garantías equivalentes.

Es también importante destacar que el artículo 11.2 de la previamente citada Ley 39/2015, relativo al uso de los medios de identificación y firma en el procedimiento administrativo, establece de forma unívoca las actuaciones en las cuales se debe requerir al interesado el uso obligatorio de un sistema de firma electrónica, siendo suficiente, para el resto, con acreditar la identidad, lo que también redundaría en la simplificación del procedimiento y en el uso proporcional de los sistemas de firma electrónica.

Por último, la también reciente Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 45.2, para el aseguramiento y la interoperabilidad de la firma electrónica entre organismos públicos, posibilita superponer un sello electrónico basado en certificado reconocido sobre aquellas firmas electrónicas generadas con sistemas que no estén basados en certificados reconocidos, para garantizar así su verificación automática por terceros.

En virtud de lo expuesto y en ejercicio de las atribuciones conferidas por el apartado I) del artículo 10.1 y el artículo 28.2 del Reglamento por el que se implantan medios electrónicos de acceso de los ciudadanos a los servicios públicos de la Universidad de Murcia y se crea la Sede Electrónica, aprobado por acuerdo del Consejo de Gobierno de fecha 6 de julio de 2009,

#### **Resuelvo:**

##### **Primero. Establecimiento del sistema de firma.**

Establecer un nuevo sistema de firma electrónica para los miembros de la comunidad universitaria que actúen como interesados en procedimientos administrativos de la Universidad de Murcia, denominado "Sistema de firma con Cuenta UM", con las siguientes características.

- El sistema se fundamenta en el uso del sistema de identificación con la cuenta de correo electrónico corporativo institucional (dominio '@um.es')

proporcionada por la Universidad de Murcia y su contraseña asociada, de acuerdo a lo previsto en el artículo 10.3 de la Ley 39/2015.

- El sistema incorpora, como medida de seguridad adicional para alcanzar un nivel de identificación sustancial, el uso de un segundo factor de autenticación, consistente en el envío de un código de un único uso generado, de forma no predecible, por la Universidad de Murcia al número de teléfono móvil asociado a la persona identificada en los sistemas de información de la propia Universidad, de acuerdo a lo previsto en el punto 4.2.5 del apartado 2 del anexo II del Esquema Nacional de Seguridad.

- El sistema incorpora, como medida de seguridad compensatoria en lo relativo a la prevención del repudio, la recolección, el almacenamiento y la protección de un conjunto de evidencias electrónicas relativas a la identificación del interesado y su actividad, como acreditación de la autenticidad de la expresión de su voluntad, de acuerdo a lo previsto en el punto 5.7.4 del apartado 2 del anexo II del Esquema Nacional de Seguridad. Son las siguientes.

- o Identificador de la transacción de firma electrónica.
- o Identificador, nombre y apellidos del interesado.
- o Fecha y hora de la transacción de firma electrónica.
- o Dirección de correo electrónico corporativo del interesado.
- o Ticket de identificación obtenido del portal de entrada de la Universidad de Murcia, una vez verificada la contraseña asociada a la dirección de correo electrónico corporativo del interesado.
- o Código de un solo uso enviado al teléfono móvil del interesado como segundo factor de autenticación.
- o Datos de navegación generados por el navegador del interesado durante la transacción de firma electrónica.
- o Datos identificativos de este sistema de firma electrónica.
- o Identificador de la aplicación responsable de la transacción de firma.
- o Identificador del trámite en el que se enmarca la transacción de firma.
- o Resumen digital del documento que se firma.

- El sistema garantiza, con un nivel de confianza sustancial, la integridad e inalterabilidad, tanto del documento firmado, como de las evidencias electrónicas recolectadas y almacenadas, mediante la superposición de un sello electrónico basado en certificado electrónico reconocido, de acuerdo a lo previsto en los artículos 10.1 y 45.2 de la Ley 39/2015.

La descripción técnica de las medidas de seguridad establecidas para este sistema de firma figura como anexo a la presente resolución.

### **Segundo. Ámbito.**

Admitir el uso de este sistema de firma por las personas físicas que, por razón de relación jurídica preexistente con la Universidad de Murcia, dispongan de cuenta de correo electrónico corporativo (dominio '@um.es'), de número de teléfono móvil asociado en los sistemas de información de la Universidad, y actúen como interesados en el procedimiento administrativo.

Con carácter general, el sistema de firma se podrá utilizar en documentos de ciudadano para los siguientes tipos de actuaciones, de acuerdo a lo previsto en el artículo 11.2 de la Ley 39/2015.

- Formular solicitudes.
- Presentar declaraciones responsables o comunicaciones.
- Interponer recursos.
- Desistir de acciones.
- Renunciar a derechos.

Los procedimientos administrativos, en el marco de los cuáles se realicen estas actuaciones, deberán estar previamente inventariados por la unidad responsable en la aplicación 'Inventario de Procedimientos y Servicios Administrativos' de la Universidad de Murcia, accesible desde la siguiente dirección: <https://inventario.um.es>

Las tipologías de las unidades documentales que sean firmadas electrónicamente en el marco de estas actuaciones, deberán estar previamente catalogadas y gestionadas en el Archivo Electrónico de la Universidad de Murcia, mediante la aplicación 'Archivo de Oficina', accesible desde la siguiente dirección: <https://archivo.um.es/oficina>

Excepcionalmente y mediante resolución del Secretario General, podrá admitirse este sistema de firma electrónica para la actuación en el ejercicio de la competencia de sus empleados públicos en procedimientos concretos. Para ello, será necesario contar con informes previos favorables de la unidad responsable del procedimiento, Asesoría Jurídica y del Área de Tecnologías de la Información y las Comunicaciones Aplicadas (ATICA), en los que se realice una evaluación de riesgos en la que se contrasten los niveles de protección frente al repudio y de reconocimiento de la identidad del empleado público por parte de terceros requeridos en el marco de dicho procedimiento, frente a los proporcionados por el sistema de firma electrónica.

#### **Tercero. Funcionamiento.**

Este sistema de firma quedará integrado en una pasarela de firma electrónica contenida en la Sede Electrónica de la Universidad de Murcia, donde el interesado en un procedimiento administrativo será redirigido, de forma automática, cada vez que se requiera la firma de un documento administrativo, realizando el proceso de firma en un mismo entorno confiable, adecuado a los requisitos del marco normativo vigente.

Desde esta pasarela, el interesado podrá revisar el contenido del documento a firmar e iniciar el proceso de firma. Durante este proceso, en primer lugar, será redirigido al portal de entrada de la Universidad para que se identifique, si no lo está ya, introduciendo su correo electrónico corporativo y contraseña asociada. A continuación, el sistema enviará un código de un único uso al teléfono móvil asociado al interesado, que deberá introducir en un formulario preparado para ello, disponiendo de tres intentos. Por último, el sistema procesará las evidencias obtenidas en el proceso, generará el documento firmado electrónicamente y redirigirá de nuevo al usuario a la aplicación gestora del procedimiento administrativo en el que participa como interesado.

#### **Cuarto. Teléfono móvil asociado.**

A los efectos de esta resolución, se considera número de teléfono móvil asociado a cada persona física el que conste como tal en las bases de datos corporativas institucionales de la Universidad de Murcia.

La solicitud de alta, modificación o actualización del número de teléfono móvil asociado solamente podrá ser presentada por la persona interesada o por quien se halle debidamente acreditada o acreditado como su representante, si dispone de poder bastante para ello, conforme a lo establecido en el artículo 5 de la Ley 39/2015, de modo que quede constancia fehaciente, a través de una de las siguientes opciones.

Para PDI y PAS:

- Mediante el acceso con certificado electrónico al servicio de Modificación de Datos Personales del Portal de Recursos Humanos: <https://rrhh.um.es/rrhh/paginas/datospersonal/>

- Mediante presentación presencial de impreso de solicitud en el Área de Recursos Humanos.

- Mediante presentación de Instancia Básica en el Registro Electrónico: <https://sede.um.es/registro/PR-SG-002>

- Mediante presentación presencial de impreso de solicitud en el Registro General o en el Registro Auxiliar de la Universidad de Murcia.

Para estudiantes:

- Mediante identificación con su Tarjeta Universitaria Inteligente (TUI) en las Secretarías Virtuales.

- Mediante presentación presencial de impreso de solicitud en la Secretaría de su Facultad o Escuela.

- Mediante presentación de Instancia Básica en el Registro Electrónico: <https://sede.um.es/registro/PR-SG-002>

- Mediante presentación presencial de impreso de solicitud en el Registro General o en el Registro Auxiliar de la Universidad de Murcia.

#### **Quinto. Creación de sello electrónico.**

Ordenar la creación del sello electrónico de órgano del "SISTEMA DE FIRMA ELECTRÓNICA CON CUENTA UM.ES", cuya titularidad corresponde a Secretaría General, como órgano responsable del sistema, y la publicación de su resolución de creación en el apartado 'Relación de sellos electrónicos utilizados por la Universidad de Murcia' de la Sede Electrónica.

Este sello será utilizado para garantizar, con un nivel de confianza sustancial, la integridad e inalterabilidad, tanto del documento firmado, como de las evidencias electrónicas almacenadas, de acuerdo a lo previsto en el apartado primero de esta resolución.

#### **Sexto. Difusión en Sede Electrónica.**

Ordenar la publicación de este nuevo sistema de firma electrónica, junto con la presente resolución, en el apartado correspondiente a sistema de firma electrónica admitidos de la Sede Electrónica de la Universidad de Murcia, en sustitución del subapartado 'Firma electrónica basada en claves concertadas'.

#### **Séptimo. Entrada en vigor.**

La presente resolución entrará en vigor tras su publicación en el Boletín Oficial de la Región de Murcia.

## ANEXO

### DESCRIPCIÓN TÉCNICA DE LAS MEDIDAS DE SEGURIDAD

El 'Sistema de firma con Cuenta UM' se fundamenta en la incorporación de una medida de seguridad adicional, para alcanzar un nivel de identificación sustancial durante las transacciones de firma de los usuarios, y una medida de seguridad compensatoria, en lo relativo a la prevención del repudio. En este anexo se describen técnicamente ambas medidas.

#### **Medida de seguridad adicional para alcanzar un nivel de identificación sustancial**

Como medida de seguridad adicional se introduce el uso de un segundo factor de autenticación, consistente en la generación de un código no predecible de 8 dígitos, que es enviado mediante mensajería instantánea al número de teléfono móvil asociado a la persona identificada.

Para la generación de este código -denominado one-time-password (OTP)- se hace uso del algoritmo 'HMAC-Based One-time Password Algorithm (HOTP)', a partir del contenido del documento a firmar y la fecha-hora del sistema. Este algoritmo se encuentra descrito en el estándar abierto RFC 4226, desarrollado por el Internet Engineering Task Force (IETF) y disponible en la siguiente dirección: <https://tools.ietf.org/html/rfc4226>

La definición matemática concreta utilizada, para obtener el código de 8 dígitos, es la siguiente:

$$\text{HOTP-Value} = \text{HOTP}(K,C) \bmod 10^d = (\text{Truncate}(\text{HMAC-SHA1}(K,C)) \& 0x7FFFFFFF) \bmod 10^d$$
, donde

- 'HOTP-Value' es el código de 8 dígitos.
- 'K' es el contenido del documento a firmar.
- 'C' es la fecha-hora del sistema.
- 'd' es el número de dígitos.
- 'Truncate' es una función de truncado que selecciona 4 bytes.
- '0x7FFFFFFF' es una máscara que se aplica al resultado de la función de truncado.
- 'HMAC-SHA1' es el algoritmo de autenticación HMAC utilizado.

#### **Medida de seguridad compensatoria para la prevención del repudio**

Como medida de seguridad compensatoria en lo relativo a la prevención del repudio se obtienen y archivan, en cada transacción de firma electrónica, el siguiente conjunto de evidencias de la actuación realizada por el usuario, como acreditación de la expresión de su voluntad.

- IdentificadorTransaccionFirma: identificador de la transacción de firma electrónica.
- Firmante: identificador (DNI o NIE), nombre y apellidos del interesado.
- FechaFirma: fecha y hora de la transacción de firma electrónica.
- Correo: dirección de correo electrónico corporativo del interesado.
- TicketService: ticket de identificación obtenido del portal de entrada.
- CódigoOtp: código de un solo uso enviado al teléfono móvil del interesado.
- PeticionPost: datos de navegación generados por el navegador del interesado durante la transacción de firma electrónica, codificados en base 64, entre los que se incluyen las cabeceras HTTP con datos identificativos sobre el

navegador del usuario y su dirección IP, junto al contenido del formulario de tramitación.

- Emisor: datos identificativos de este sistema de firma electrónica en la Universidad de Murcia.

- IdentificadorAplicacion: identificador de la aplicación responsable de la transacción de firma electrónica.

- IdentificadorTramite: identificador del trámite en el que se enmarca la transacción de firma electrónica.

- ResumenDigitalDocumento: resumen digital del contenido que se firma en la transacción y algoritmo utilizado para realizar el cómputo.

Todas estas evidencias se integran en una única estructura normalizada en lenguaje XML denominada 'EvidenciasFirmaCuentaUM'. Se puede observar un ejemplo a continuación.

```
<cu:EvidenciasFirmaCuentaUM xmlns:cu="urn:umu:eadmin:firma:cuentaum:schema"
```

```
  Id="firmaCuentaUM-2017-01-23-13-56-53-1450972801">
```

```
<cu:IdentificadorTransaccionFirma>96f8b6ff-e263-4c48-a2cb-
```

```
  04b11b42277a</cu:IdentificadorTransaccionFirma>
```

```
<cu:Firmante>
```

```
  <cu:Identificador>000000001R</cu:Identificador>
```

```
  <cu:Nombre>JUAN</cu:Nombre>
```

```
  <cu:Apellidos>MURCIANO ESPAÑOL</cu:Apellidos>
```

```
</cu:Firmante>
```

```
<cu:FechaFirma>2017-01-23T13:56:53.175+01:00</cu:FechaFirma>
```

```
<cu:Correo>correo@um.es</cu:Correo>
```

```
<cu:TicketService>ST-446480-UCPcXC60TAxleepxd6GY0-
```

```
  elephas31.um.es</cu:TicketService>
```

```
<cu:CodigoOtp>70292057</cu:CodigoOtp>
```

```
<cu:PetitionPost>UmVxd...KICB9Cg==</cu:PetitionPost>
```

```
<cu:Emisor>Universidad de Murcia (Resolución SG-XX/2017)</cu:Emisor>
```

```
<cu:IdentificadorAplicacion>REGISTRO</cu:IdentificadorAplicacion>
```

```
<cu:IdentificadorTramite>PR-000059</cu:IdentificadorTramite>
```

```
<cu:ResumenDigitalDocumento>
```

```
  <cu:Valor>7bVq8Igl4UvEWpbqZtuNfxxeZd+TBeY8x8HHnH2oxKk=</cu:Valor>
```

```
  <cu:Algoritmo>SHA-256</cu:Algoritmo>
```

```
</cu:ResumenDigitalDocumento>
```

```
</cu:EvidenciasFirmaCuentaUM>
```

Para garantizar la integridad e inalterabilidad de la firma, esta estructura XML se incluye, junto con el contenido a firmar, en un único documento administrativo electrónico en formato XAdES-T (con sello de tiempo), autenticado de forma automatizada con el sello electrónico basado en certificado reconocido 'SISTEMA DE FIRMA CON CUENTA UM.ES' de la Universidad de Murcia, de acuerdo a la Política de Firma Electrónica y Certificados de la Administración General del



<ds:KeyInfo>

...

<ds:KeyName>**CN=SISTEMA DE FIRMA ELECTRONICA CON CUENTA UM.ES,  
serialNumber=Q3018001B,OU=SELLO ELECTRONICO,O=UNIVERSIDAD DE MURCIA,  
C=ES**</ds:KeyName>

</ds:KeyInfo>

...

</ds:Signature>

</du:DocUniversitario>

Este documento es archivado en el Archivo Electrónico y soporta sus diferentes procesos de gestión documental, de acuerdo a la Política de Gestión de Documentos Electrónicos de la Universidad de Murcia, aprobada en Consejo de Gobierno de 13 de febrero de 2014, y publicada en el apartado de 'Política de Gestión de Documentos Electrónicos' en Sede Electrónica, disponible en la siguiente dirección: <https://sede.um.es/sede/gestion-documental>.